Solution Brief

Getting Increased Value out of Your Fabric Connect Network

With Fabric Remote Switch Port Analyzer (RSPAN)

Executive Summary

Fabric Remote Switch Port Analyzer (RSPAN) is a feature that is currently available on Extreme VSP and Universal Switching Platforms. It is used to send a copy of network packets seen on the specified ports (source ports) to other specified ports (destination ports).

Fabric RSPAN can significantly reduce costs and simplify the deployment of many third-party solutions such as:

- Performance monitoring solutions
- IDS/IPS solutions
- IoT discovery and security solutions
- VoIP call recording solutions
- Packet capture/analyzer tools such as Wireshark

This paper provides an overview of Fabric RSPAN, how it differs from industry standard approaches, how it can be used and how it works with Integrated Application Hosting to provide simpler on-board packet capture/packet analyzer capabilities to facilitate troubleshooting.

Introduction to Fabric Connect

Extreme Networks' Fabric Connect technology (based on the industry standard Shortest Path Bridging) is redefining networking to match the speed of today's digital era. Long wait times required for network additions or changes and the rigid design constraints of legacy networks have made it challenging for network IT teams to move at the speed of the business. Fabric Connect eliminates these delays and enables our customers to deploy networks that are far more agile; enabling rapid application deployment and seamless services provisioning - while also improving the reliability, stability and security of the network.

With almost a decade of in-service deployments, Fabric Connect is incredibly feature rich. Fabric RSPAN is a well deployed feature that enables port and traffic mirroring capabilities over a Fabric Connect network.

What is Port and Traffic Mirroring (SPAN/RSPAN)?

Port mirroring is used on a network switch or a router to send a copy of network packets seen on the specified ports (source ports) to other specified ports (destination ports). With port mirroring enabled, the packets can be monitored and analyzed. Port mirroring is applied widely, to analyze and debug data or diagnose errors on their networks without affecting the packet processing capabilities of the network devices.

Traffic mirroring copies only the specified traffic that matches a certain configuration or Access Control List (ACL) rule to the destination port for analysis and monitoring. While port mirroring copies every packet that passes through the interface to the monitoring device, with traffic mirroring, only the selected or matched traffic are sent to the monitoring device.

Port and traffic mirroring can either be local or remote. With local mirroring traffic from a source port is mirrored and sent to a destination port on the same switch. With remote port and traffic mirroring, the source and destination ports are not on the same device.

The Value of Port and Traffic Mirroring (SPAN/RSPAN)

The biggest value of port and traffic mirroring, is that rather than purchasing and deploying inline sensors or traffic splitters, the network itself can duplicate network traffic and direct the copied traffic a specific destination that includes connectivity to a specialized security appliance or performance monitoring tool. Deploying inline sensors or traffic splitters can not only be complex, it can also be costly. Therefore, using the network, which is already in place anyway, to duplicate and send traffic simplifies operations and can provide significant cost savings for an organization.

What is Fabric RSPAN?

Fabric RSPAN represents the way to do port, VLAN and traffic mirroring in a Fabric Connect enabled network. With the Fabric-based implementation port, VLAN or flow-based traffic is mirrored to a Fabric Connect service (which is called an Independent Service Identifier or I-SID). This mirrored traffic can be sent to one or more switches within the Fabric Connect network for analysis by central or distributed collector/analyzers.

In a Fabric Connect network, the source device where the traffic is mirrored into an I-SID, is known as a Mirroring BEB (Fabric Edge Node) and the remote device where the network traffic analyzer is connected for mirrored traffic analysis is known as Monitoring BEB (Fabric Edge Node). There can be multiple Mirroring BEBs and Monitoring BEB's in a Fabric Connect network.

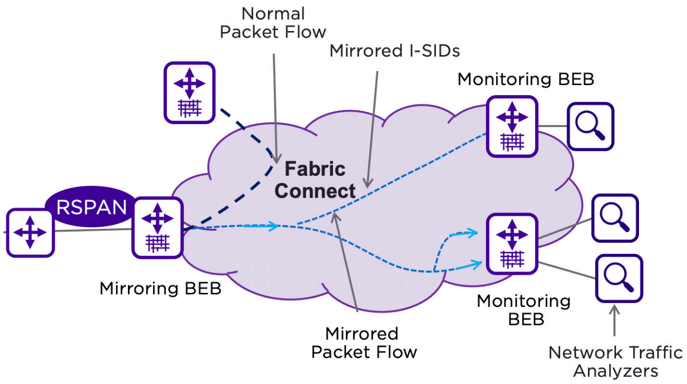

Figure 1: Fabric RSPAN deployment

What Makes Fabric RSPAN Unique?

There are distinct advantages of the Fabric RSPAN features when comparing it to RSPAN deployed in a traditional (non-Fabric based network).

- **Simplified configuration** with RSPAN in a traditional network, mirrored traffic is copied over a special-purpose VLAN. This VLAN requires manual administration hop by hop from the source to the destination. With Fabric RSPAN, traffic is copied to a Fabric Connect service or I-SID which is dynamically established once the source and destinations are configured, eliminating much of the time consuming and error prone configuration common in traditional networks.
- **Efficient replication** with Fabric RSPAN, the mirrored traffic is sent as L2 multicast traffic and can thereby be replicated to multiple monitoring ports at any desired location in the Fabric Connect network. In addition, multiple mirrored I-SIDs (or Fabric Connect services) can be monitored on a single monitoring port.
- **Ability to apply QoS** with Fabric RSPAN, QoS for the mirrored traffic is configurable.

What is Encapsulated Remote SPAN (ERSPAN) and How Does Fabric Connect RSPAN Compare?

Encapsulated remote SPAN brings generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains. Fabric Connect RSPAN also allows for traffic and port mirroring to be extended across Layer 3 domains; in fact, as stated earlier, traffic can be replicated to any fabric edge device (BEB) regardless of where it resides in the fabric network.

What Are the Use Cases for Fabric RSPAN?

There are numerous use cases for implementing Fabric RSPAN. These include:

- **Reduce costs in the deployment of performance monitoring systems:** Many performance monitoring systems require the use of in-line sensors or traffic sniffers to collect traffic that is then sent to an analytics system for in-depth traffic analysis. When deploying these systems, it is possible to reduce costs by using the network to replicate and send traffic to the performance monitoring system, thereby reducing or even eliminating the need for sensors/traffic sniffers.

- **Reduce costs in the deployment of IDS/IPS and IoT security systems:** In addition to performance monitoring systems, many IDS/IPS systems and IoT security solutions also require the deployment of in-line sensors and/or traffic sniffers. Again, using the network to copy and send traffic to the system itself can simplify and reduce the costs of deploying these security systems.
- **Reduce costs in the deployment of VoIP call recording solutions:** Organizations who are deploying VoIP call recording solutions can choose to leverage Fabric RSPAN to mirror and send traffic to a centralized call recorder that can then use intelligent packet capturing to find and record all the RTP (audio) steams. This may be a simpler and more cost-effective solution than deploying call recording software at every workstation.
- **Remote management and configuration:** RSPAN functionality can be very useful for remote management and configuration. When it is inconvenient to physically get to a remotely deployed switch to perform configuration updates, you can use RSPAN to replicate and span the traffic from one port to the remotely deployed port, rather that driving to a specific location to perform the configuration updates.
- **General Network Debugging/Troubleshooting/Security Compliance:** Fabric RSPAN is a critical OAM feature that can help organizations monitor and analyze traffic for real-time troubleshooting, security analysis and/or anomaly detection. It is typically used with applications such as WireShark, Splunk, PerfSONAR and others.

Integrated Application Hosting to Further Simplify Troubleshooting and Security Compliance

To further simplify the deployment of packet capture/analyzer tools for the purposes of debugging, troubleshooting and/or security compliance, select Fabric Connect-enabled switches support a feature called Integrated Application Hosting. This means that rather than having to deploy a separate server to host select applications such as Wireshark (or others), these applications can be deployed on the switch itself as a separate virtual machine. Within the switch, the Guest VM application has its own dedicated memory and CPU resources to ensure consistent performance. In addition, 10-20 Gig internal ports are used to interconnect the switch operating system to the integrated hosted application. Traffic mirroring is supported on the internal ports.

Having an on-board packet capture application, distributes the functionality closer to the suspected issue. This means if there is a network issue, such as packet loss, that is occurring on a specific switch, it is possible to RSPAN traffic to the Wireshark (or other) application on the Guest VM of the switch. This provides direct visibility as to what is happening on that switch. The captured files can be stored on the Guest VM and then emailed out of the Guest VM using the Chrome Browser via any email client of choice.

Having on-board packet capture capabilities can not only accelerate mean time to repair for suspected issues, it can also simplify the overall deployment, reducing the need for using external PCs.

Summary

Fabric RSPAN can not only provide simplicity as well as significant cost savings, it also allows networking IT teams to expand the role of the network to provide additional value to your organization's security and application's teams. For the technical details on how to implement this specific feature within your Fabric Connect network, please reach out to you Extreme Networks representative.

Extreme networks

http://www.extremenetworks.com/contact